FC-BGP:
Towards Secure Inter-domain Routing and Forwarding via Verifiable Routing Commitments

Zhuotao Liu
Tsinghua University

On behalf of other coauthors: Ke Xu, Xiaoliang Wang, Qi Li and Jianping Wu

https://datatracker.ietf.org/doc/draft-wang-idr-frameworkoffcbgp/
Scope and Outline

• Recap on the design goals and problem space of FC-BGP
• FC-BGP protocol specification
  • FC-BGP path attribution definition
  • BGP best path selection in case of FC-BGP
  • FC-BGP generation for different peers
• FC-BGP deployment status update
Recap: Design Goals

Control Plane

**Full Deployment:** FC-BGP can guarantee that any BGP path authenticated by our protocol is a real path announced by the on-path ASes, i.e., it is infeasible for the adversary to claim that a forged BGP path is authenticated.

**Partial Deployment:** FC-BGP is compatible with the native BGP, and incrementally deployable (i.e., FC-BGP provides strictly positive security benefits for BGP paths whose on-path ASes are not fully deployed.

Data Plane

Unwanted traffic (including traffic with spoofed source or sent via undesired path) can be detected by the upgraded ASes.
Recap: Verifiable Routing Commitments

Suppose AS B receives a BGP update $P: S \leftarrow A \leftarrow B$, AS B uses the following Forwarding Commitment to publicly certify its routing intent over the next hop to AS C

$$F_{\{A, B, C, P\}} = \{ H(A, B, C, P)Sig_B \ || \ A \ || \ B \ || \ C \},$$

(i) FC-BGP adopts a per-pathlet validation scheme for validating BGP updates, instead of the per-path validation scheme used in BPGsec, which has two benefits

1) Same security guarantees as BGPsec in full-deployment, but with much lower path validation overhead in dynamic networks, like the Internet

2) (Strictly) more security benefits than BGPsec in case of partial deployment

(ii) The routing commitments do not cause extra disclosure of routing policies.
### FC-BGP Attribute

<table>
<thead>
<tr>
<th>Flags</th>
<th>Type</th>
<th>FCList Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FCList</td>
</tr>
</tbody>
</table>

#### Format of FC path attribute

- **Flags (1 octet):** The current value is `0b11010000`, representing the FC attribute as **optional, transitive, partial, and extended-length**.
- **Type (1 octet):** The current value is TBD, which is waiting for the IANA assignment.
- **FCList Length (2 octets):** The value is the total length of the FCList in bytes.
- **FCList (variable length):** The value is a sequence of FCs, in order.

<table>
<thead>
<tr>
<th>Previous Autonomous System Number</th>
<th>Current Autonomous System Number</th>
<th>Next-hop Autonomous System Number</th>
<th>Subject Key Identifier</th>
<th>Algorithm ID</th>
<th>Flags</th>
<th>Signature Length</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Format of an individual FC

- **Previous Autonomous System Number (PASN, 4 octets):** The AS number of the previous AS.
- **Current Autonomous System Number (CASN, 4 octets):** The AS number of the current AS.
- **Next-hop Autonomous System Number (NASN, 4 octets):** The AS number of the next hop AS.
- **Subject Key Identifier (SKI, 20 octets):** The public key of the signing party.
- **Algorithm ID (1 octet):** It indicates algorithms for hashing and signing.
- **Flags (1 octet):** Its value MUST be 0.
- **Signature Length (2 octets):** It indicates the signature length in bytes.
- **Signature (variable length):** The signature content and order are `Signature=ECDSA(SHA256(PASN, CASN, NASN, Prefix))`. 
FC-BGP does not modify the “AS Path” attribute. Instead, it defines a new transitive path attribute so that the legacy ASes can forward this attribute to its peers without changing any protocol.

Thus, FC-BGP is natively compatible with the BGP. This is different from BGPsec which replaces the AS path attribute with a new “Secure path” attribute.
Processing an FC-BGP UPDATE Message

Upon receiving a BGP UPDATE message with FC path attribute specified, an FC-BGP-upgraded AS will perform three steps:

(i) Verify the AS-Path attribute.
(ii) BGP best path selection
(iii) Update the FC path attribute and continue advertising the BGP route to the next hop.
Verify the AS-Path Attribute

- Upon AS D receives an UPDATE message from AS K, it retrieves the FC path attribute and extracts the FC list, and verify the FC signed by AS A and AS B.
- AS C and AS K are legacy ASes: they simply ignore the FC-BGP path attribute.
BGP Best Path Selection

FC-BGP adds two priority rules in the second and third positions

- Local preference is the highest priority
- Full path validation
- Partial path validation
- Shorter AS-Path
- Other attributes with lower priority than the AS-Path length

See the proof of the lemma in the preprint: https://arxiv.org/abs/2309.13271
FC Generation for Different Peers

(i) FC-BGP speakers must generate different UPDATE messages for different peers.

(ii) When an AS (e.g., AS E) prefers to announce multiple route prefixes, it needs to generate different UPDATE messages for each route prefix.
  
  • It extends the FC List by appending its own FC to the original FC List.

An example for receiving multiple UPDATE messages (AS E)
FC-BGP Deployment Status

• Deployment Principle: Strategically deploying FC-BGP capable devices to avoid universally upgrading all routers (which is infeasible).

• Current deployment status:
  • We first build an overlay in China, crossing multiple ASes to test the basic functionality of FC-BGP.
  • The next step is to deploy our FC-BGP capable prototype with real ASNs and prefixes, and start to prorogate actual FC-BGP update messages through these networks.
Conclusion

✓ FC-BGP is a novel secure inter-domain routing system that can simultaneously authenticate BGP routing updates and validate data plane forwarding in an efficient and incrementally-deployable manner.

✓ FC-BGP is built upon a unified primitive, named Verifiable Routing Commitment, to enhance the security of control plane routing and data plane forwarding.

✓ FC-BGP is fully compatible with BGP, and incrementally deployable by offering strictly positive security benefits in partial deployment. FC-BGP has the same security guarantee as BGPsec in full deployment, while imposing much lower verification overhead.

See additional details: https://www.ietf.org/archive/id/draft-sidrops-wang-fcbgp-protocol-00.html
Thank You!
**Key takeaways:**

- Non-colluding assumption (two compromised ASes do not collude)
- Any path that can be validated by strategically combining FCs is a legitimate path that is announced by the on-path ASes
- Caveat: replay attack

See additional details in our preprint: https://arxiv.org/abs/2309.13271
Data Plane Forwarding Validation

Key takeaways:

- By propagating the verifiable routing commitment in FC-BGP backwards, the on-path ASes can learn the desired forwarding path on the data plane, based on which they can choose to enforce certain policies (such as filtering unwanted traffic).
Quantified Security Benefits in Partial Deployment

- We sort the ASes according to the number of their neighbors.
- Given a deployment rate $r$, we select the top $r$ ASes to deploy FC-BGP.
- Then for all the BGP updates in the CAIDA dataset, we check whether the adversary can hijack a BGP update by constructing a forged but shorter AS path.
- We report the hijack rate for different deployment rates.

Key takeaways:

FC-BGP provides strictly more security benefits than BGPsec in partial deployment.
Key takeaways

- FC-BGP is compatible with BGP so that the authenticated pathlets can be passed along the path.
- Lemma: if the consecutive deployment is sufficiently long, the entire path is secured even if some of the on-path ASes are not upgraded
Recap: Problem Statement

The current Internet inter-domain routing has vulnerabilities in both the control plane and the data plane.

- Control plane: no built-in mechanism to verify the BGP announcements
- Data plane: the actual data forwarding path is not consistent with the BGP path
Recap: Problem Space

Assumption and Scope:
(i) ASes have access to an Internet-scale trust base, namely Resource Public Key Infrastructure (RPKI), that stores authoritative information about the mapping between AS numbers and their owned IP prefixes, and their public keys.
(ii) Multi-path forwarding (for instance due to traffic engineering / ECMP) is not considered to be a violation of data plane security.

Adversary:
(i) The adversary can intercept all the BGP update messages (also referred to as BGP announcements) in the network.
(ii) On the control plane, the adversary can launch path manipulation attacks (i.e., hijacking a BGP path with a shorter path).
(iii) On the data plane, the adversary can spoof source addresses and/or reroute the traffic to desired ASes.
(iv) Two compromised ASes will not collude.